Attribute Based Access Control For Protecting Programmable Logic Controllers

Shwetha Gowdanakatte[*], Indrakshi Ray[*], Siv Hilde Houmb[#]

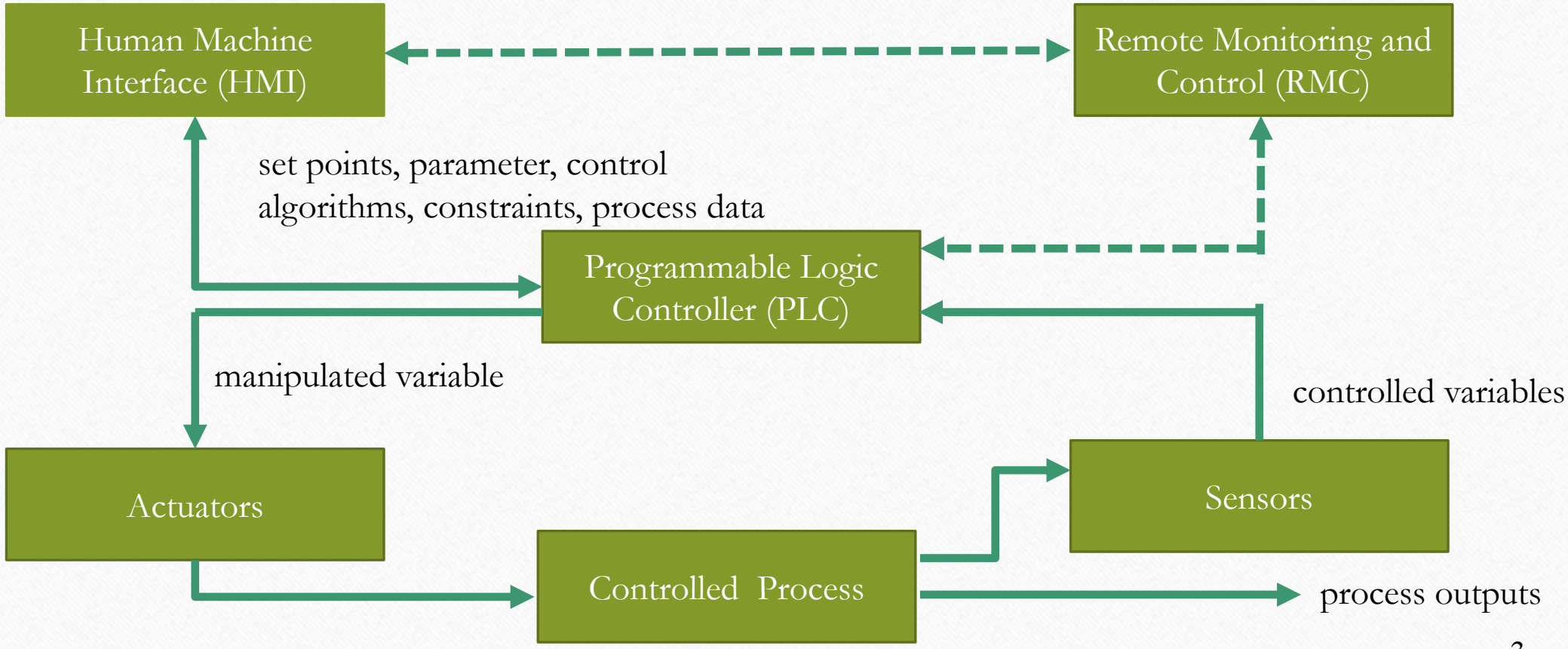
[*]Colorado State University

[#]Norwegian University of Science and Technology

Overview

- Introduction
- Background
- Related Work
- Our Method
- Future Work
- References

Industrial Control Systems



ICS Cyber Attack and Vulnerability Statistics

Cyber Attack Statistics

- ICSs targeted in 2021: 39% based on Kaspersky report
- Major cause: flaws in the authentication and access control
- Oldsmar water system attack: Feb 2021: Unauthorized remote access to HMI
- 75% of water utilities had connections to OT. 75% of loss of control (DoS). 50% loss of safety: Drago's report

Vulnerability Statistics

- 41% Increase in the number of ICS in vulnerabilities based on Claroty report in 2021
- 70% are rated as critical
- 90% are low attack complexity
- 61% are remotely exploitable
- 74% do not need user privileges
- Most of the PLC and HMI vulnerabilities are related to authorization and access control

Programmable Logic Controllers

Siemens S7-1500

- Engineering Framework: Totally Integrated Automation (TIA) portal
- Communication Protocol: S7-P3

Rockwell Compact Logix

- Engineering Framework: Studio 5000
- Communication Protocol: Common Industrial Protocol (CIP)

Authentication and Access Control in ICS

PLC

- Authentication: password based
  - 2-step authentication required for accessing the components: software, firmware, and communication modules
- Access control: Discretionary access control for CPU access

HMI

- Authentication: password based
- Access Control: Role Based Access Control (RBAC)

RMC

- Authentication: password-based protection for remote access
- Access Control: Role Based Access Control (RBAC) for remote operations

Recent Vulnerabilities

S7-1500

CVE	Description
CVE-2019-10943	Sending crafted TCP packets to modify the running code
CVE-2020-15782	Violation of memory protection by sending crafted TCP packets to Port 102
CVE -2021-37185	DoS attack by sending crafted TCP packets to TCP port 102
CVE-2019-10929	Man-in-the-middle attack

Compact Logix

CVE	Description
CVE-2021-1392	Obtain a CIP password and add an authorized admin user
CVE-2021-22681	Bypass authentication to impersonate Studio 5000
CVE-2016-9342	Crafted TCP Packets

Related Work (1)

Message Authentication Codes [2]

- Proposes authenticated data exchanges through Message Authentication Codes (MAC) between the ICS components
- The control software is constructed with MAC
- Addresses Man-in-the-middle attack from unauthorized devices
- Does not address Man-in-the-middle from rogue ICS components
- Requires design change
- Vendor specific implementation
- Does not provide centralized solution

[2] D. Adrian-Vasile, G. Béla, and H. Piroska. 2018. Enabling authenticated data exchanges in industrial control systems. 1–5. https://doi.org/10.1109/ISDFS.2018.8355337 Last accessed 12 December 2021.

Related Work (2)

Role Based Access Control For ICS

- Industries are moving towards RBAC mechanism for ICS [13]
- Rockwell [4], Honeywell [8], other PLC/HMI vendors provide RBAC
- Existing implementations are vendor specific and do not provide centralized solution
- RBAC alone is not sufficient for event driven complex ICS
- Safety critical operations depend on the ICS status and environmental conditions

- [13]: F. Santiago, A. Javier, and A. Saioba. 2019. A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach, Vol. 19. https://doi.org/10.3390/s19204455.
- [4]:Rockwell Automation. 2021. FactoryTalk Security System Configuration Guide. https://literature.rockwellautomation.com/idc/groups/literature/documents/qs/ftsec-qs001_-en-e.pdf. Last accessed 21 November 2021.
- [8] Honeywell ACS Labs. 2014. RBAC Driven Least Privilege Architecture For Control Systems. https://www.osti.gov/servlets/purl/1124080/. Technical Report (2014). Last accessed 20 June 2021.

Related Work (3)

ABAC For ICS [16]

- Implements ABAC for accessing an ICS process
- Does not address access related vulnerabilities at component level
- Incorporates XACML standard that does not support dynamic policies

[16]: E. Yalcinkaya, A. Maffei, and M. Onori. 2017. Application of Attribute Based Access Control Model for Industrial Control Systems. International Journal of Computer Network and Information Security 9 (2017), 12–21. https://doi.org/10.5815/ijcnis.2017.02.02

Our Approach: Attribute Based Access Control

Attribute Based Access Control

- Provides fine-grain policies by combining user, object and environmental attributes
- Good for open ended environments
- Standardizations
  - eXtensible Access Control Markup Language (XACML)
  - NIST Next Generation Access Control (NGAC)

XACML

- Developed for collaborative environments
- Extensible and is an XML encoded language
- Can specify access control policies, access control requests, and access control decisions

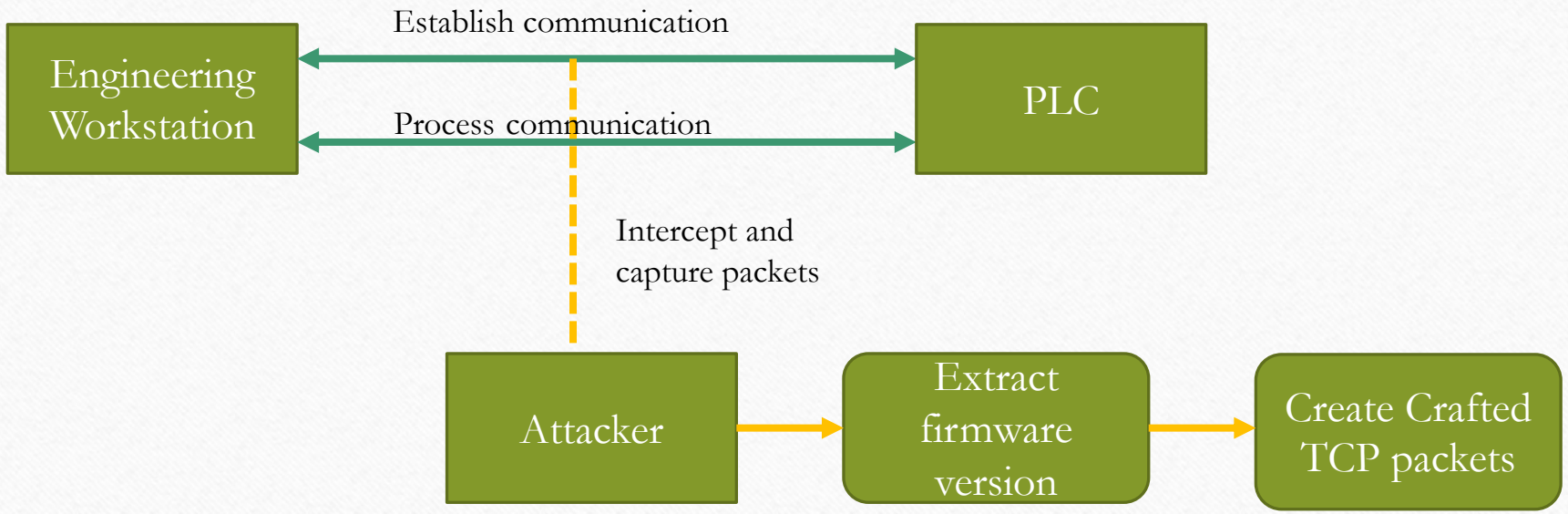
NGAC

- Policies consist: Users, Resources, Operations
- Does not express policy through rules but using relations
- Policy management is more streamlined
- Support dynamic policies

Threat Model(1)

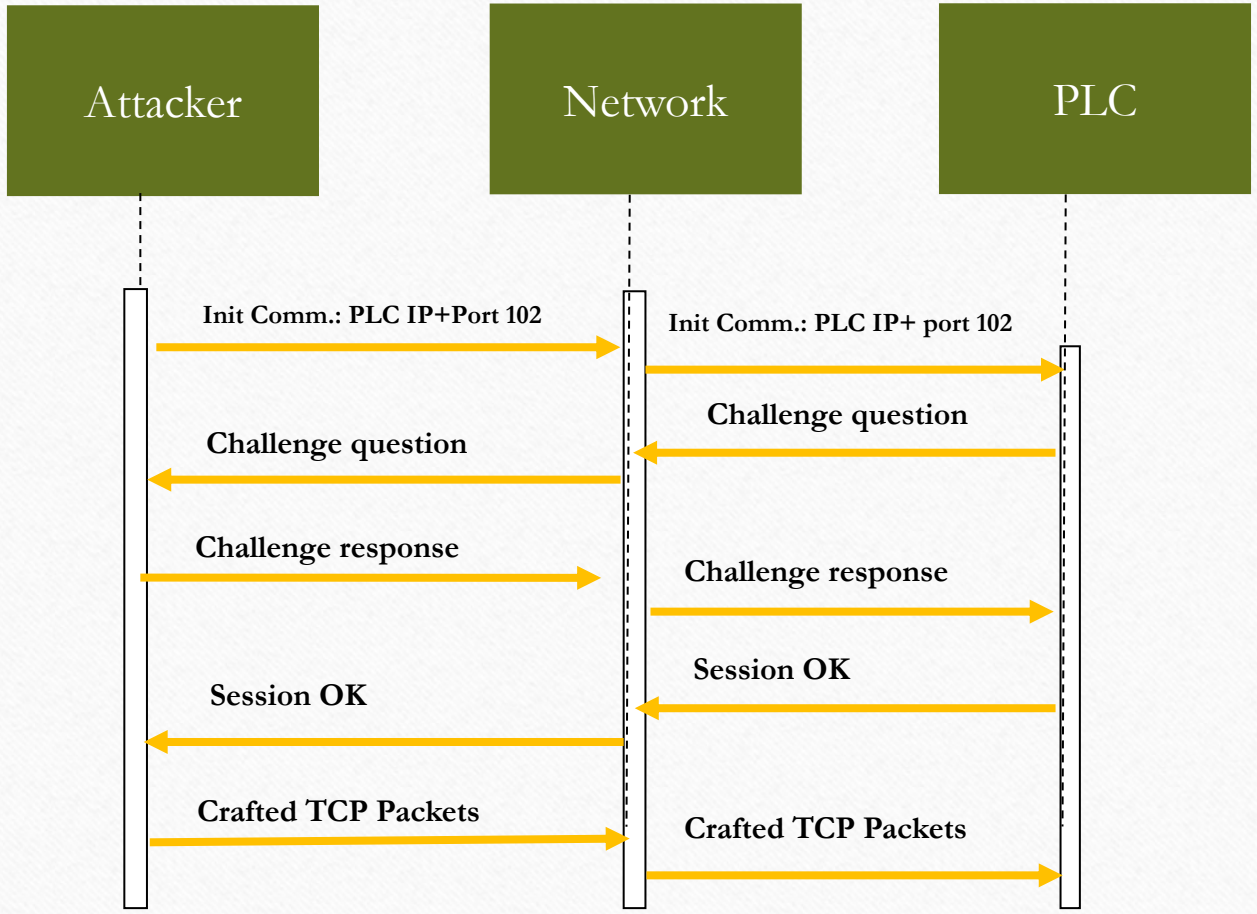
Attack with CVE: CVE-2020-15782

Attack Phase-1

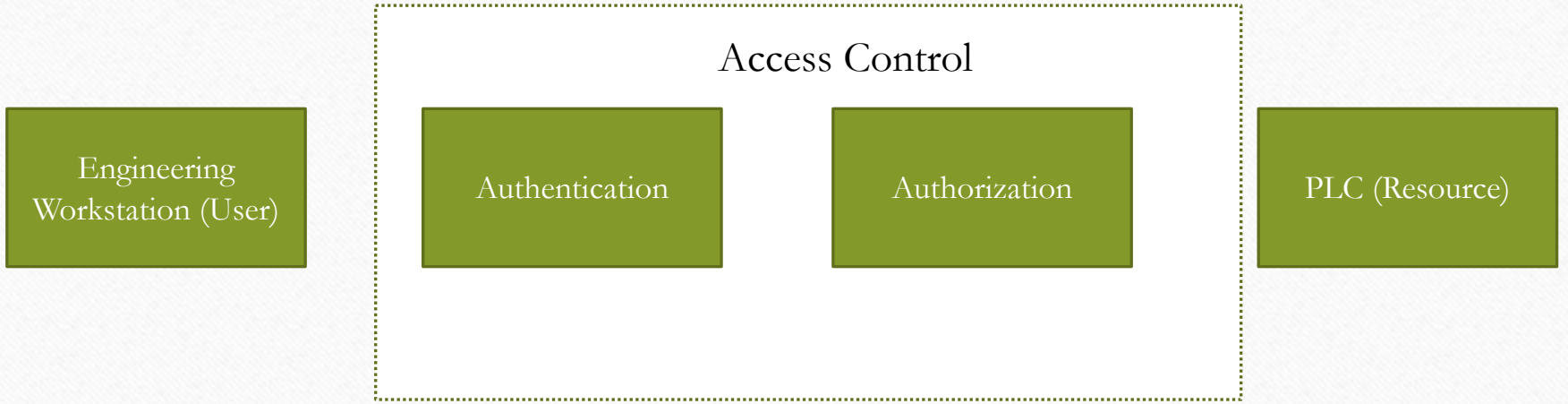


Threat Model(2)

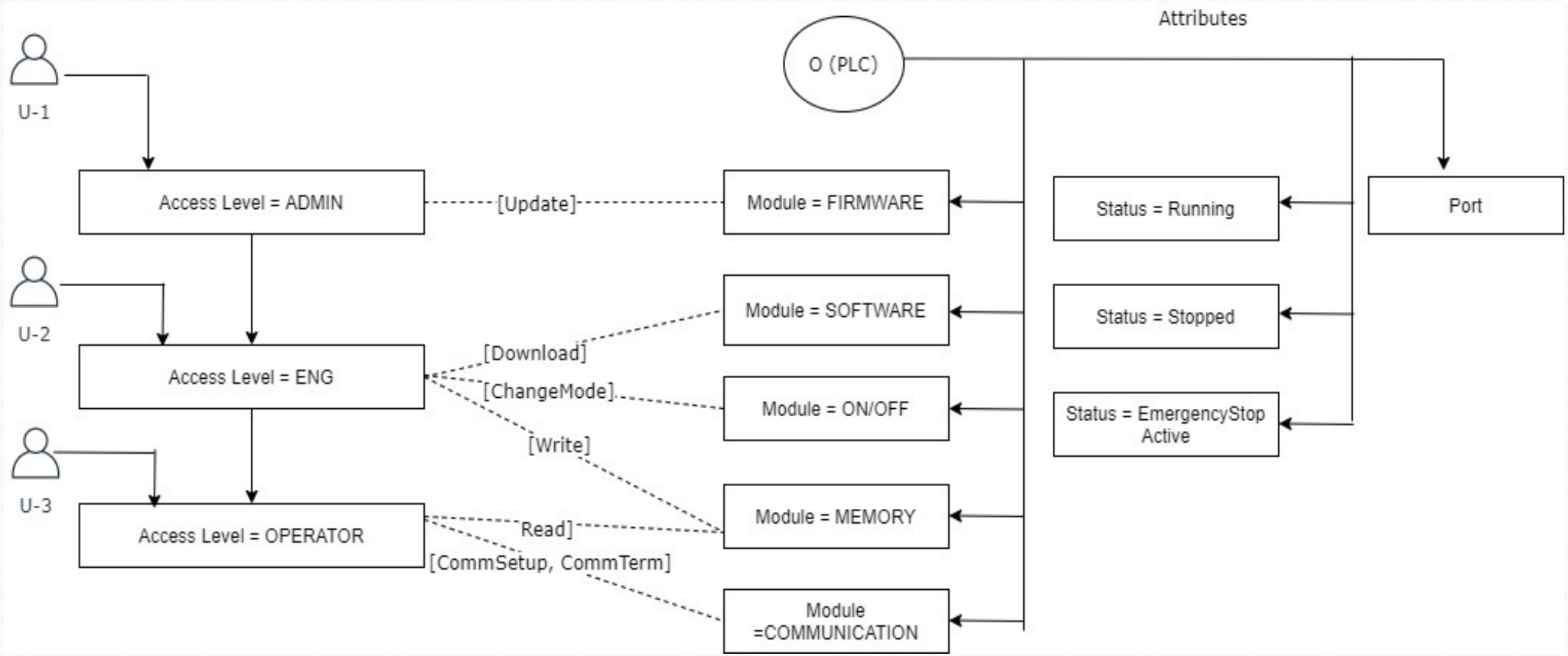
Attack Phase-2



Our Framework



Application of ABAC for PLC: NIST-NGAC Model



Application of ABAC for PLC: Policy formalization

Each policy is expressed as a tuple

<{User Attribute}, {Resource Attribute},{Environmental Attribute},{operation}>

User Attributes

- Access Level = {Operator, Engineer, Administrator}
- Device ID

Resource (PLC) Attributes

- Module = {Software, Firmware, Communication, Memory, ON/OFF}
- Status = {Stopped, Running, Emergency Stop Active}
- Operating Mode = {Program, Test, Error, Remote}
- Port

Environmental Attributes

- User Access Time
- User Access Location

Application of ABAC for PLC: Policy formalization

Communication Setup Policy

<{(User.AccessLevel ∈ {Operator, Engineer, Administrator), (User.Device = "Equip 21L OrgABC")}, {(PLC.OperatingMode = Remote)}, {(Env. Access Time = 700 − 16 : 00EST), (Env. Access Loc = OrgABC.local")}, {CommSetup}>

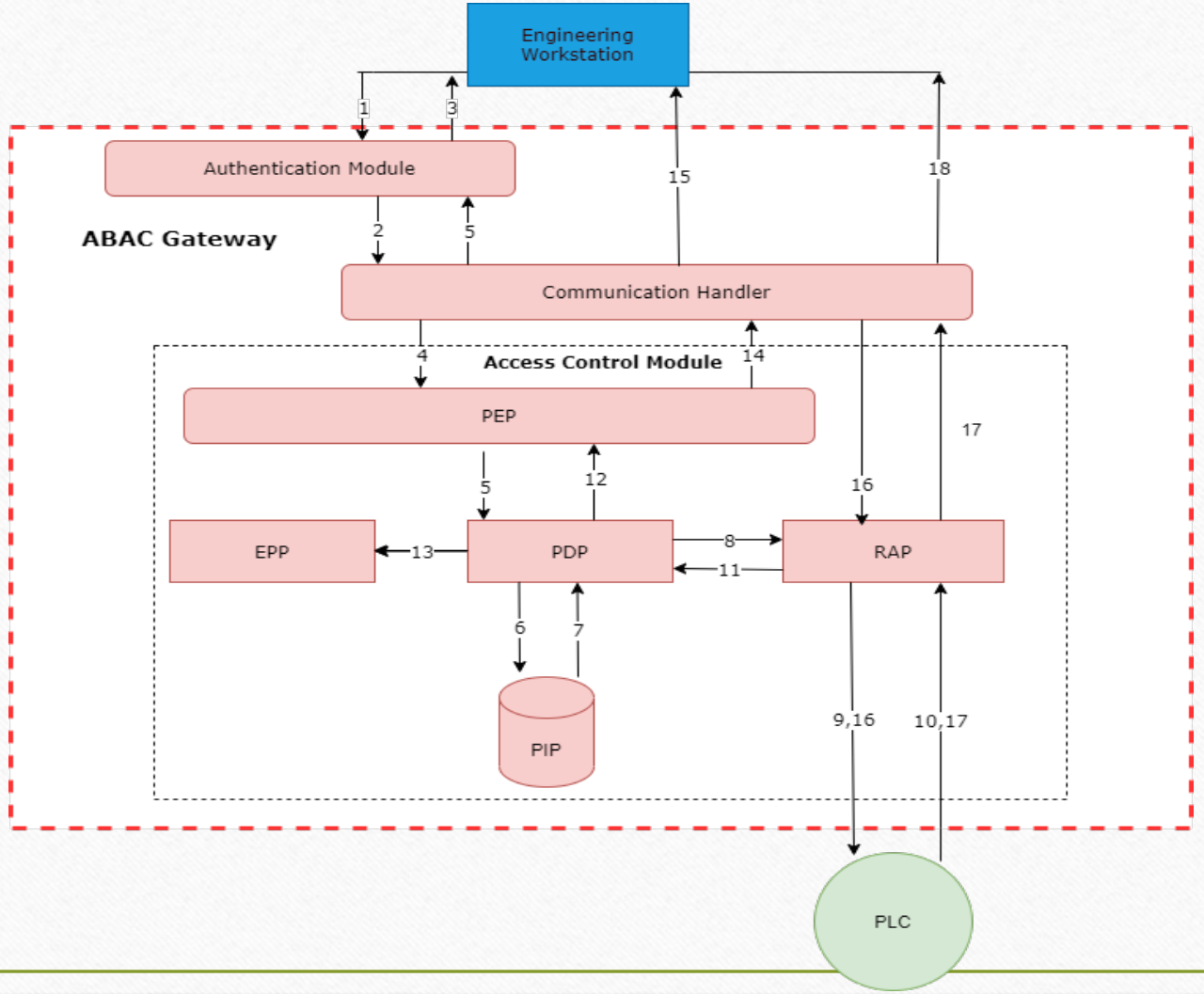
Memory Write Policy

<{(User.AccessLevel ∈ {Engineer, Administrator})}, {(PLC.OperatingMode = Program), (PLC.Status= Stop)}, {True}, {WriteMem}>

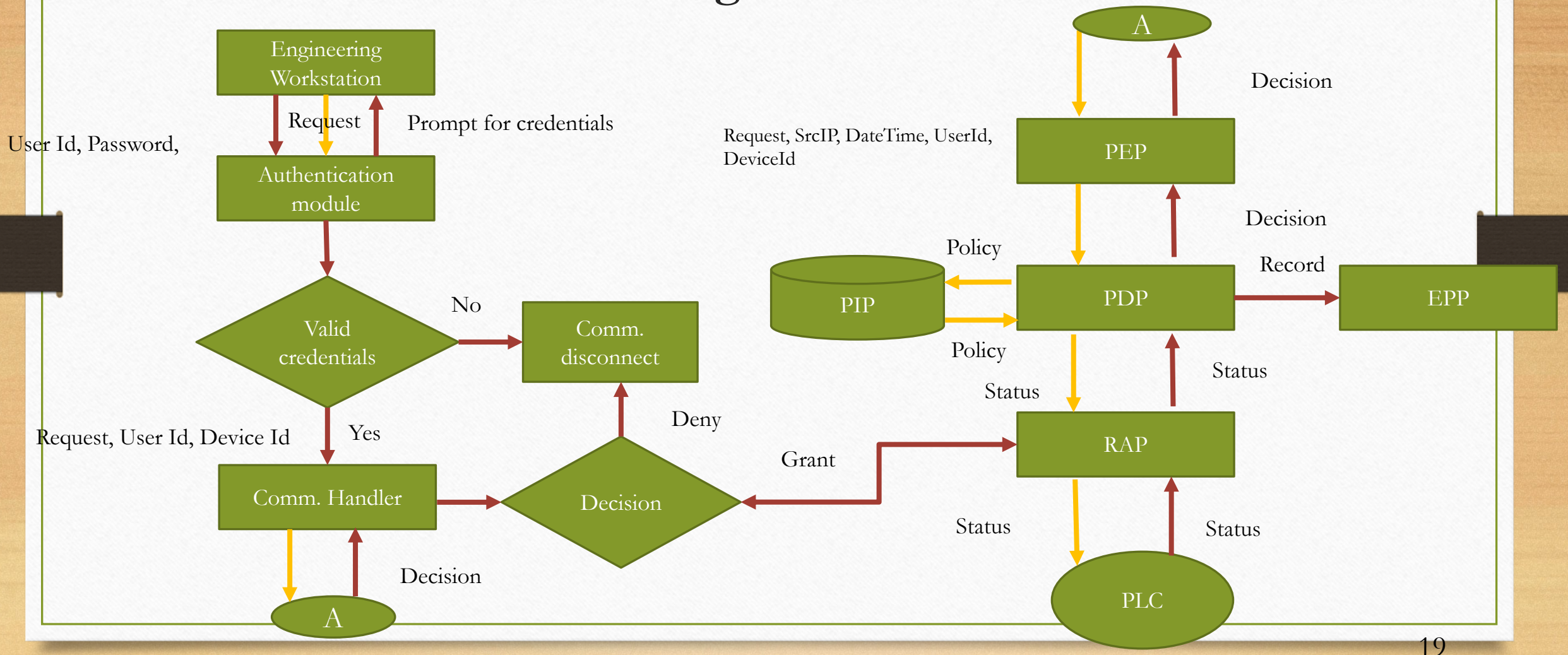
Firmware Update Policy

<{(User.AccessLevel ∈ {Administrator)}, {(PLC.OperatingMode = Program), (PLC.Status= Stop)}, {True}, {Update}>

Application of ABAC for PLC: Architecture

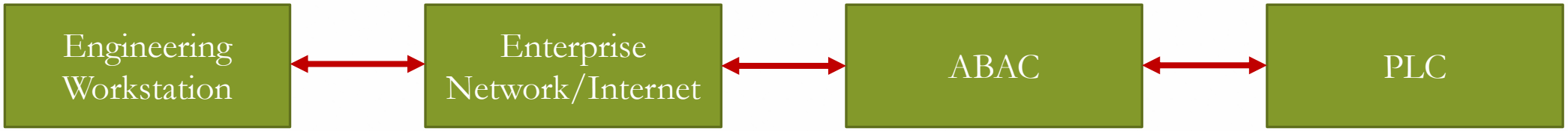


Communication between Engineering Workstation and PLC through ABAC



Security Analysis (1)

Communication Architecture



Assumptions

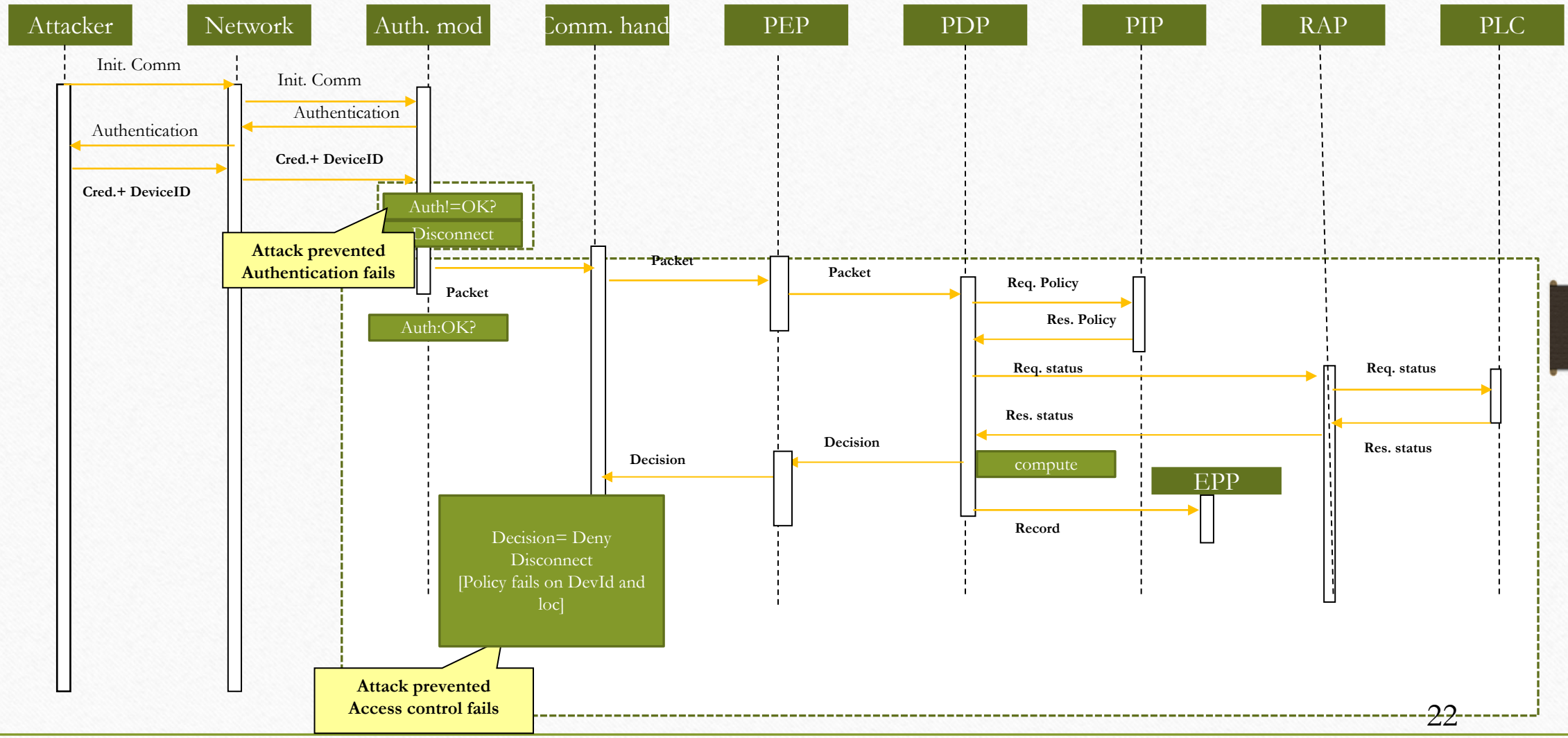
- The ABAC module is trusted and tamper resistant
- PIP and EPP databases in ABAC module are secure and tamper resistant
- The communication between the ABAC and the PLC is protected
- User credentials and attributes are encrypted

Security Analysis (2)

Protection provided by ABAC module

- Protection against integrity attack
- Protection against repudiation attack
- Protection against availability attack (DoS)
- Protection against elevation of privilege

Security Analysis (3)



Future work

- Verification and analysis of CVEs for all major PLCs
- Determine which CVEs are related to access control issues
- Implementation and enforcement of ABAC model as a centralized solution for a given ICS
- Future implementation includes distributed ICS

Acknowledgement

- NSF
- NIST
- Cyber Risk Research
- Statnett
- AMI
- ARL

References

[1] A. Adeen, Y. Hyunguk, and A. Irfan. 2021. Empirical Study of PLC Authentication Protocols in Industrial Control Systems. 383–397. https://doi.org/10.1109/SPW53761.2021.00058 Last accessed 12 December 2021.

[2] D. Adrian-Vasile, G. Béla, and H. Piroska. 2018. Enabling authenticated data exchanges in industrial control systems. 1–5. https://doi.org/10.1109/ISDFS.2018. 8355337 Last accessed 12 December 2021.

[3] M. Aftab, Z. Qin, S. Zakria, S. Ali, Pirah, and J. Khan. 2018. The Evaluation and Comparative Analysis of Role Based Access Control and Attribute Based Access Control Model. In *International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*. 35–39. https://doi.org/10. 1109/ICCWAMTIP.2018.8632578

[4] Rockwell Automation. 2021. FactoryTalk Security System Configura- tion Guide. https://literature.rockwellautomation.com/idc/groups/literature/ documents/qs/ftsec-qs001_-en-e.pdf. Last accessed 21 November 2021.

[5] E. Biham, S. Bitan, A. Carmel, A. Dankner, U. Malin, and A. Wool. 2019.

[6] Rogue Engineering Station Attacks on Simatic S7 PLCs. https://i.blackhat.com/USA-19/Thursday/us-19-Bitan-Rogue7-Rogue-Engineering-Station-Attacks-On-S7-Simatic-PLCs.pdf/. Last accessed 5 July 2021.

[7] T. M. Chen and S. Abu-Nimeh. 2011. Lessons from Stuxnet. *Computer* 44, 4 (2011), 91–93. https://doi.org/10.1109/MC.2011.115

[8] D. Ferraiolo, R. Chandramouli, D. Kuhn., and V. Hu. 2016. Extensible Access Con- trol Markup Language (XACML) and Next Generation Access Control (NGAC).
In *ACM International Workshop*. 13–24. https://doi.org/10.1145/2875491.2875496

References

[9] Honeywell ACS Labs. 2014. RBAC Driven Least Privilege Architecture For Control Systems. https://www.osti.gov/servlets/purl/1124080/. *Technical Report* (2014). Last accessed 20 June 2021.
[10] NIST. 2019. https://nvd.nist.gov/vuln/detail/CVE-2019-10943/. Last accessed 1 July 2021.
[11] NIST. 2019. https://nvd.nist.gov/vuln/detail/CVE-2019-10952. Last accessed 1 Jan 2022.
[12] NIST. 2021. https://nvd.nist.gov/vuln/detail/CVE-2020-15782/. Last accessed 1 July 2021
[13] NIST. 2021. https:https://nvd.nist.gov/vuln/detail/CVE-2021-22681. Last accessed 1 Jan 2022.
[14] F. Santiago, A. Javier, and A. Saioba. 2019. A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach, Vol. 19. https://doi.org/10.3390/s19204455.
[15] Shodan. [n. d.]. https://www.shodan.io/. Last accessed 23 July 2021.
[16] Unknown. 2018. Packet Sniffing in Python. https://www.uv.mx/personal/angelperez/files/2018/10/sniffers_texto.pdf/. Last accessed 15 July 2021.
[17] E. Yalcinkaya, A. Maffei, and M. Onori. 2017. Application of Attribute Based Access Control Model for Industrial Control Systems. *International Journal of ork and Information Security* 9 (2017), 12–21. https://doi.org/10.jcnis.2017.02.02

Thank you!

Questions?